HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,921	12/14/2000	Kyung-hee Kang	1337.1028/MDS	5815

21171 7590 01/07/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/735,921	KANG ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for R ply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Final rejection

1. Claims 1, and 3-6 are pending in this office action,

2. The amended specification received on 09/09/2004 is accepted.

3. Applicant's arguments with respect to claims 1, and 4-6 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5 Claims 1, and 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al. (Van, U.S Patent No. 5,699,431) in view of in view of Micali (U.S. Patent No. 5,717,758) and of Micali (Micali II, U.S. Patent No. 6,487,658), and in further view of Kocher (Pub. No.: US 2002/0188843 A1)

As per claim 1, Van teaches in the field of certificate management for public-key cryptography. In particular, it is directed to a new method for managing lists of revoked certificates (certificate revocation lists), by partitioning them into smaller segments thereby allowing the maximum potential size of any one segment to be kept arbitrarily small, and allowing efficient processing of lists according to revocation reasons. (Col. 1 lines 6-15, Fig. 5)

a) the certificate policy statement for the CRL by determining the distribution interval of the CRL; (Fig. 5, col. 5 lines 26 – 66; address list) In order to manage CRL it is inherited that certificate policy statement is registered.

b) to issue the certificate according to the registered certificate policy statement; (Col. 3 lines; (Fig. 5, Col. 3 lines 29-48) In order to issue a certificate it is inherited that structure of the certificate is set.

c) attesting the certificate by applying the distribution point mechanism according to the distribution interval to the CRL; (Fig. 5, Col. 3 lines 29-48)

d) revoking the certificate by using the distribution point to revise the CRL displayed. (Fig. 5, col. 3 lines 20-48)

wherein the step a) includes the steps of:

a1) the hash to manage the CRL based on the number of the expected subscribers; (Col. 5 lines 26-41)

a2) defining the subject name (SUBJECT NAME) of the essential items constituting the certificate as the input value of the hash function; (Fig. 1-3)

Van fails to explicitly describe defining the number of nodes in the DIT; and Calculating the distribution interval of the CRL by using the hash function and variables.

However, it would be obvious to one skilled in the art at the time of the invention to perform defining the number N of the nodes in the directory information tree (DIT); and Micali teaches computing a one-way hash by executing function on the CRL for segmented CRL; (Col. 9 lines 65-col. 10 lines 34)

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the invention was made to combine the teachings of Van and Micali because distribution point mechanism for CRL allows one to prove whether a given certificate is valid or revoked without providing the validity of all certificates and provides more efficient certificate revocation information.

The combination of Van and Micali teach all the limitations as shown above.
Van and Micali fail to explicitly describe setting the value of the variable (crl_dp_flag) for the CRL according to the distribution interval.

However, Micali II discloses a segmented CRL (SCRL) with distribution intervals. (Col. 10 lines 58- col. 11 lines 28)

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the invention was made to combine the teachings Micali II, and the combination of Van and Micali because SCRL mechanism would minimize the amount of "unwanted information" for each of the above queries, and reduce downloading time.

Van, Micali, and Micali II do not explicitly teach an equation ((Vmax – Vmin) / N) = I.

However Kocher discloses a3) calculating the distribution interval of the CRL by using following hash function H() and an equation ((Vmax – Vmin) / N) = I (Kocher Page 2 par. 0025), wherein V represents a value obtained by inputting the subject name (SUBJECT NAME) to the hash function H() (Kocher Page 2 par. 0025; serial number), Vmax is a maximum value

among a plurality of V, Vmin is a minimum value among a plurality of V, N is the number of the nodes and I is the distribution interval of the CRL (Kocher Page 2 par. 0025);

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the invention was made to employ the teachings Kocher within the combination system of Van, Micali and Micali II because it would allow to produce distribution intervals.

As per clam 6, it has similar limitation as claim 1; therefore, it is being rejected under the same rationale.

As per claim 3, the combination of Van, Micali, Micali II, and Kocher teach the invention as discussed above. In addition Micali teaches

b1) retrieving the subject name (SUBJECT NAME) of the subscriber as the input of the hash function or skipping according as the certificate policy statement sets the distribution point to be applied to the CRL (crl dp flag=yes) or not; (Col. 9 lines 25-43)

b2) calculating the hash value (Vtmp) for the retrieved subject name; (Col. 6 lines 26-38; col. 9 lines 26-col. 10 lines 35)

b3) obtaining the interval value (n) including the hash value to complete the distinguished name (DN) of the CRL upon revoking the corresponding certificate; (col. 13 lines 56 - col. 14 lines 68) and

b4) issuing the certificate of the subscriber by setting the structure of the certificate by using the DN information of the CRL and the DN information of the certifying agency issuing the CRL. (Col. 5 lines 46 – col. 6 lines 20)

As per claim 4, the combination of Van, Micali, Micali II, and Kocher teach the invention as discussed above. In addition Micali teaches

c1) preparing a phrase concerning the certificate of the subscriber according to the subject name (SUBJECT NAME) of the subscriber; (Col. 2 lines 49-col. 3 lines 49)

c2) requesting the certificate of the subscriber from the directory server by using the phrase to retrieve the information of the corresponding structure from the certificate downloaded according to the subject name(SUBJECT-NAME); (Col. 5 lines 1-69)

c3) requesting the CRL designated the corresponding DN from the directory server according to the retrieved information; (Col. 3 lines 29-col. 4 lines 45)

c4) retrieving the serial number of the subscriber by checking the duration of the effective time based on the CRL; (Fig. 5, col.1 lines 6-67, col3 lines 55-col. 4 lines 65) and

c5) invalidating or validating the subscriber's certificate according as the serial number is included in the CRL or not. (Col. 3 lines 14-55)

As per claim 5, the combination of Van, Micali, Micali II, and Kocher teach the invention as discussed above. In addition Micali teaches

d1) revising the subscriber's certificate requested for revocation in the database (DB) or skipping according as the certificate policy statement applied to the subscriber sets the distribution point to be applied to the CRL (crl dp flag=yes) or not; (Col. 5, lines 27-57)

d2) revising the CRL retrieved according to the information of the structure of the revised subscriber's certificate through the corresponding database; (Col. 3 lines 29-49)

d3) retrieving the reason of revoking the certificate from the packet received from the subscriber by detecting the serial number of the revised subscriber's certificate; (Col. 3 lines 13-49) and

d4) writing the CRL revised to include the serial number of the subscriber's certificate (Fig. 5, col. 3 lines 56-col. 4 lines 3, Col. 6 lines 8-15) and the code representing the reason of revocation into the node of the DIT managed by the directory server. (Col. 5 lines 16-20, col. 6 lines 8-15, Fig. 4-7)

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703 305 0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703 305 9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER